

日本国特許庁  
JAPAN PATENT OFFICE

JC997 U.S. PTO  
09/989772  
11/20/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。 #5

This is to certify that the annexed is a true copy of the following application as filed  
with this Office

出願年月日

Date of Application:

2000年11月30日

出願番号

Application Number:

特願2000-365915

出願人

Applicant(s):

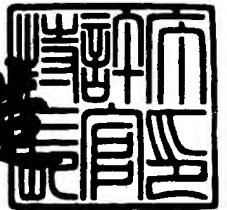
アジレント・テクノロジー株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 5月11日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



出証番号 出証特2001-3040197

BEST AVAILABLE COPY

【書類名】 特許願

【整理番号】 40004102

【あて先】 特許庁長官 殿

【国際特許分類】 G08B 25/00

【発明者】

    【住所又は居所】 東京都八王子市高倉町 9 番 1 号 アジレント・テクノロジー株式会社内

    【氏名】 山本 健司

【発明者】

    【住所又は居所】 東京都八王子市高倉町 9 番 1 号 アジレント・テクノロジー株式会社内

    【氏名】 村田 耕

【特許出願人】

    【識別番号】 000121914

    【氏名又は名称】 アジレント・テクノロジー株式会社

【代理人】

    【識別番号】 100105913

    【弁理士】

    【氏名又は名称】 加藤 公久

【手数料の表示】

    【予納台帳番号】 042745

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

    【包括委任状番号】 9912029

【プルーフの要否】 要

【書類名】明細書

【発明の名称】セキュリティシステム

【特許請求の範囲】

【請求項 1】

所定の場所に固定されたカメラ装置により得られた侵入者検知情報を、通信回線を通してユーザに通報するセキュリティシステムにおいて、

前記所定の場所に対応して前記カメラ装置が複数台設置され、

前記カメラ装置及びインターネット回線手段を含む前記通信回線に、通信のために接続可能な通信装置と、前記インターネット回線手段を介して前記通信装置に接続可能なサーバ手段とを有し、

前記カメラ装置のそれぞれは前記所定の場所における侵入者を常時監視しつつ、該侵入者を検知したときにのみ前記通信装置との接続を確立して前記通信装置に異常信号及び画像データを送り、

前記通信装置は、前記異常信号を受信したときにのみ前記サーバ手段との通信を確立して、受信した前記画像データを所定の単位にまとめて前記サーバ手段に送信するよう構成されることを特徴とするセキュリティシステム。

【請求項 2】

前記通信装置は、前記画像データの前記所定の単位を前記サーバ手段に送信した後前記画像データを自動的に消去するよう構成されることを特徴とする請求項 1 のセキュリティシステム。

【請求項 3】

前記画像データの前記所定の単位は、前記カメラ装置の複数台のうちの特定の一つに対して時間経過を追って得られる複数の画像データを含むことを特徴とする請求項 1 のセキュリティシステム。

【請求項 4】

前記カメラ装置と前記通信装置との相互接続は、電源線を使用するか又は無線により行われることを特徴とする請求項 1 のセキュリティシステム。

【請求項 5】

前記サーバ手段は、前記画像データによる画像情報を特定のウェブサイト上に

提供することを特徴とする請求項 1 のセキュリティシステム。

【請求項 6】

前記サーバ手段は、前記画像データを受信したときに予め登録した端末に対して通報を行うこと特徴とする請求項 1 のセキュリティシステム。

【請求項 7】

前記通報は、インターネット回線手段を使用して行われることを特徴とする請求項 6 のセキュリティシステム。

【請求項 8】

前記カメラ装置は音声情報も検出し、該音声情報による音声データを前記画像データと合わせて送信できることを特徴とする請求項 1 のセキュリティシステム。

【請求項 9】

前記サーバ手段は、ウェブサーバ手段及びデータベースサーバ手段を含むことを特徴とする請求項 1 のセキュリティシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、セキュリティシステムに関し、特にホームセキュリティのためのシステムにして、外部からの不法な侵入者を検知し、その情報を必要とされる者に対して通報する通信機能を備えたセキュリティシステムに関する。

【0002】

【従来の技術及び発明の解決すべき課題】

従来のホームセキュリティシステムの多くは、防犯が必要とされる場所に設置された赤外線等を利用する各種センサにより侵入者の有無を検知して、異常が認められる場合にはそれを通報するシステムとなっている。例えば、不法な侵入者が現れた場合には、センサがこれを検知して、公衆電話回線（携帯電話システムを含む）又は専用回線等を使って集中監視センタへと異常信号を送信する。異常を確認した集中監視センタの監視員は、現場に警備員を緊急に派遣するなどの措置をとる。

## 【 0 0 0 3 】

しかし、このシステムにおける最も大きな問題は、センサからの信号のみでは侵入者の存在を正確に知ることができない点である。赤外線センサ等のセンサのみによれば、誤報が生じる件数も少なくはなく、この場合にも異常信号が集中監視センタに送られる。集中監視センタでは現実には侵入者が現れたときと同じ措置をとることになるのでその措置は無駄なものとなってしまう。このことは、システムの運営を高価なものとしてしまう原因となる。

## 【 0 0 0 4 】

侵入者の存在を正確に把握するために、センサ情報に加えて画像で監視する方法も検討されている。その一例が特開平 1 1 - 2 2 4 3 8 3 号公報に記載される。このシステムでは、防犯が必要とされる場所に設置されたカメラからの情報を P H S システムを使ってユーザ端末上に表示させる機能を有する。このシステムも改善すべき問題を内包する。

## 【 0 0 0 5 】

第 1 の問題は、このシステムによれば、一見即座に情報が伝えられるようであるが、必要とされる情報以外に情報を含むものであって、結果としてユーザが侵入者の存在を確実に知るまでには余分の時間が必要となってしまう点である。これにより、情報を迅速に必要とするユーザは不便を感じることになり、情報の伝達に必要なとされる通信費用も割高になってしまう。第 2 の問題は、監視が必要とされる場所に複数のカメラを設置した場合の制御が困難である点である。上述の公報には、監視が必要とされる場所に設置される監視カメラは一つである。従来複数の監視カメラを用いての通報を行うことのできるシステムは存在しなかった。第 3 の問題は、画像記憶に関するものである。上述の公報に開示される技術によれば、カメラ画像には時間遅延を伴ったビデオ映像としてのみ記憶される。この場合、必要なビデオ画像を即座に活用することは困難であり、また記憶容量にも制限がある。また上述の公報に記載されているように、監視される場所と同じ場所に画像記憶装置が配置されることは防犯上必ずしも好ましくない。

## 【 0 0 0 6 】

そこで本発明は、上述の問題に鑑みて、正確な情報の効率的な伝達及び活用を

比較的単純な構成で且つ低コストで実現することのできるセキュリティシステムを提供することをその目的とする。

【0007】

【課題を解決するための手段】

本発明は、所定の場所に固定されたカメラ装置により得られた侵入者検知情報を、通信回線を通してユーザに通報するセキュリティシステムにおいて、前記所定の場所に対応して前記カメラ装置が複数台設置され、前記カメラ装置及びインターネット回線手段を含む前記通信回線に、通信のために接続可能な通信装置と、前記インターネット回線手段を介して前記通信装置に接続可能なサーバ手段とを有し、前記カメラ装置のそれぞれは前記所定の場所における侵入者を常時監視しつつ、該侵入者を検知したときにのみ前記通信装置との接続を確立して前記通信装置に異常信号及び画像データを送り、前記通信装置は、前記異常信号を受信したときにのみ前記サーバ手段との通信を確立して、受信した前記画像データを所定の単位にまとめて前記サーバ手段に送信するよう構成されることを特徴とするセキュリティシステムを提供する。

【0008】

好ましくは、前記通信装置は、前記画像データの前記所定の単位を前記サーバ手段に送信した後に前記画像データを自動的に消去するよう構成される。

【0009】

好ましくは、前記画像データの前記所定の単位は、前記カメラ装置の複数台のうちの特定の一つに対して時間経過を追って得られる複数の画像データを含む。

【0010】

好ましくは、前記カメラ装置と前記通信装置との相互接続は、電源線を使用するか又は無線により行われる。

【0011】

好ましくは、前記サーバ手段は、前記画像データによる画像情報を特定のウェブ上に提供する。

【0012】

好ましくは、前記サーバ手段は、前記画像データを受信したときに予め登録し

た端末に対して通報を行う。

【 0 0 1 3 】

好ましくは、前記通報は、インターネット回線手段を使用して行われる。

【 0 0 1 4 】

好ましくは、前記カメラ装置は音声情報も検出し、該音声情報による前記音声データを前記画像データと合わせて送信できる。

【 0 0 1 5 】

好ましくは、前記サーバ手段は、ウェブサーバ手段及びデータベースサーバ手段を含む。

【 0 0 1 6 】

即ち、本発明のセキュリティシステムによれば、ユーザにとって監視が必要とされる場所に複数のカメラ装置及び通信手段が設けられる。セキュリティモードがオンとされると、複数のカメラ装置は、その場所の特定位置を監視するよう動作する。各カメラ装置は、それ自体が動き検出機能を有し、侵入者の動きが検出されたときにのみ異常信号及び必要な画像情報を通信手段に提供する。カメラ装置による画像を主要な判断基準としているので、従来よりも誤報の件数を減らすことができる。通信手段はカメラ装置からの異常信号を受けたときのみインターネット回線を使って情報センタとなるサーバ手段に接続され、このときカメラ装置からの情報もサーバ手段に提供される。画像は異常情報と同時に又は送信完了後に送られる。このとき、サーバ手段は、ユーザが予め選択した方法によりユーザ又は他の者への通知を自動で行わせることができる。ユーザは通知のあったときにサーバ手段にアクセスして、異常に関する詳細な情報を画像として確認できる。これにより、システムは比較的簡易にして安価に実現可能なものとなり、ユーザにとっても使いやすいものとなる。

【 0 0 1 7 】

通知を受けたユーザは、サーバ手段を介して通信手段にアクセスして、各カメラからの画像情報他を確認できる。この際、ユーザはユーザ端末から各カメラ装置を制御できるよう構成され得る。このとき、サーバ手段は、制御のために必要となる通信回線のうち公衆電話回線に必要とされる料金が最小となるように適当

なインターネットサービスプロバイダを選択することができる。

【 0 0 1 8 】

上述した他の者への通知は、自動のものでなく、ユーザからのアクセスにより初めて行われるようにも設定可能である。このとき、サーバ手段は、事前に与えられた情報、異常信号受信の際に受けた情報、ユーザからのアクセスがあったときにユーザから与えられた情報等から、適当な接続先を選択することも可能であり、その通信確立の際にも、前段落の説明と同様にして、適当なインターネットサービスプロバイダを選出できる。

【 0 0 1 9 】

【発明の実施の形態】

以下に添付図面を参照して本発明の好適実施形態となるセキュリティシステムの構成について詳細に説明する。

【 0 0 2 0 】

図 1 には、本発明の好適実施形態となるセキュリティシステム 1 0 0 の概略図が示される。このセキュリティシステム 1 0 0 は、インターネット回線 8 0 を利用し、サーバ手段 1 0 を中心に構成したものであることが理解される。サーバ手段 1 0 はウェブサーバ 1 1 及びデータベースサーバ 1 2 を含む。一方、各家庭の建物等の監視されるべき場所 2 0 0 には、複数台のカメラ装置 2 1、2 2、2 3 及び少なくとも一つの通信装置 2 0 が設けられる。セキュリティシステム 1 0 0 がホームセキュリティとして使用される場合は、各カメラ装置 2 1、2 2、2 3 は各家庭の建物の内外の必要な箇所に配置される。カメラ装置は図中には 3 台が示されるが、その数に限るものではなく、必要に応じてその数は増減される。なお図 1 には更にセンサ 2 9 が設けられる。センサ 2 9 からの情報については、特に詳述しないが、やはりサーバ手段 1 0 (のデータベースサーバ 1 2) まで送られ、状況の判断に補助的に利用される。

【 0 0 2 1 】

後述するように、カメラ装置 2 1、2 2、2 3 は、通信装置 2 0 と通信可能とされる。カメラ装置 2 1、2 2、2 3 と通信装置 2 0 との間の通信手段は、例えば電源線等の通常の家家庭に配設されている線や、Bluetooth<sup>TM</sup>等の無線通信手段



が利用され得る。一方、通信装置 2 0 は、ダイヤルアップ接続等により公衆電話回線等 7 1 及びインターネットサービスプロバイダ 8 1 を介してサーバ手段 1 0 のウェブサーバ 1 1 に接続され得る。また、サーバ手段 1 0 は、その鏡像の関係にして、ユーザ端末 2 8 に対しても、インターネット回線 8 0、インターネットサービスプロバイダ 8 2、公衆電話回線等 7 2 を介して接続可能とされる。それぞれの通信の確立及びその動作については後述する。

#### 【 0 0 2 2 】

図 2 には、システムの 4 種類の設定モードが示される。この設定モードの切替えは、通信装置 2 0 で行なわれ得る。「オフモード」は、管理者がその場所にいる場合であり、監視の必要が無く、カメラ装置 2 1、2 2、2 3 による監視が行われない状態を意味する。「セキュリティオンモード」は、管理者不在となりカメラ装置 2 1、2 2、2 3 による監視が必要とされる場合に設定されるモードである。例えば、管理者が外出する際に、このモードに設定すると、外出までに必要とされる時間の経過後に、このモードの動作が開始され、カメラ装置 2 1、2 2、2 3 による監視が開始される。他の 2 つのモード「時刻指定監視モード」及び「メッセージ送信モード」は必ずしも必要なものではなく、追加の作用を提供するものである。これらについても後述するが、その前に「セキュリティオンモード」での作用について詳細に説明する。なお、セキュリティシステム 1 0 0 には他の追加のモードも設定し得る。

#### 【 0 0 2 3 】

図 3 には、監視されるべき場所 2 0 0 に設置されたカメラ装置 2 1、2 2、2 3、及び通信装置 2 0 の更に詳細な構成が示される。カメラ装置 2 1、2 2、2 3 は、全て同じ構成を有するので、カメラ装置 2 1 を代表させて説明する。カメラ装置 2 1 は、カメラ受像部 4 1、データ処理部 4 2、メモリ部 4 3、送受信部 4 4、及び制御部 4 5 を有する。また、通信装置 2 0 は、第 1 の送受信部 9 1、データ処理部 9 2、メモリ部 9 3、及び第 2 の送受信部 9 4 を有する。またカメラ装置 2 1、2 2、2 3 は、付加的にマイクロフォン等を含む音声検知手段 4 9 を有し、画像に加えて音声をデータとして取り込み、これを画像データと合わせた監視データとし得る。従って、以後では説明の便宜上、画像データとして説明

するが、この画像データは音声データを含むことがあり得る。

【 0 0 2 4 】

システムが「セキュリティオンモード」に設定されると、カメラ装置 2 1、2 2、2 3 のそれぞれは通信装置 2 0 から動作開始の信号を受けて監視動作を開始する。カメラ装置 2 1、2 2、2 3 は、このとき通信装置 2 0 との通信状態をオフにしつつ単独で動作するか、又は消費電力を下げた状態で通信装置 2 0 との間で準備的な信号交換のための通信を行う。

【 0 0 2 5 】

カメラ装置 2 1 を代表させて、その動作について説明する。カメラ装置 2 1 内のカメラ受像部 4 1 は受像した画像を画像データにしてデータ処理部 4 2 に送る。データ処理部 4 2 は、特定の動きをする物体を検出する動き検出機能を有する。即ち、カメラ受像部 4 1 に、動いている侵入者の像が写ったとき、対応する画像データを受けたデータ処理部 4 2 では、その画像データ中の動きに関する情報から侵入者の存在を検知することができる。

【 0 0 2 6 】

カメラ装置 2 1 は、データ処理部 4 2 で侵入者の存在を検知した場合に、初めて通信装置 2 0 との通信接続を確立し、送受信部 4 4 から通信装置 2 0 の第 1 の送受信部 9 1 に向けて異常信号を送信する。侵入者の存在を検知する前後での画像データが必要に応じて静止画としてメモリ部 4 3 に記憶されるが、その全部又は一部は、異常信号と合わせて又は異常信号を送った後で通信装置 2 0 に向けて送信される。

【 0 0 2 7 】

第 1 の送受信部 9 1 でカメラ装置 2 1、2 2、2 3 の少なくとも一つから異常信号を受けた通信装置 2 0 は、第 2 の送受信部 9 4 でサーバ手段 1 0 へ接続されるべく、インターネットサービスプロバイダ（I S P）8 1 への接続を確立するよう動作するが、その一方でデータ処理部 9 2 において受信した画像データの整理を行う。画像データは、異常信号を送信してきた各カメラ装置 2 1、2 2、2 3 ごとに経時的な静止画の画像データとして整理される。通信接続が確立すると、通信装置 2 0 は、サーバ手段 1 0 に向けて、異常信号と整理された画像データ

とを送る。異常信号と画像データとは合わせて又は別個に送られるが、いずれの場合にも、カメラ装置 21、22、23 のそれぞれに対応したデータ形式で送られる。サーバ手段 10 に送られた画像データは、データベースサーバ 12 に保存される。なお、カメラ装置 21、22、23 及び通信装置 20 に一時的に記憶される画像データは、それらが適正に次段の装置に送られた後に消去され得る。

## 【0028】

サーバ手段 10 に異常信号が送られると、ユーザが希望する場合には、サーバ手段 10 から異常があったことを知らせるための自動通知が行なわれる。通知手段としては、やはりインターネット回線 80 を使ったユーザ端末 28 へのメール配信のための電子メール手段、電話会社 65 を経由した携帯電話手段又は固定位置にある電話 66（図 1 参照）等がある。これにより、ユーザは即座に不在時の異常を知ることができる。この場合の通知先は、1 個所に限らず複数箇所としても良い。

## 【0029】

データベースサーバ 12 に送られた画像データは、ウェブサーバ 11 による特定のウェブサイトアクセスし、認証を受けることによって外部から確認可能とされる。即ち、異常を知ったユーザは、インターネット回線 80 に入り、ウェブサーバ 11 にアクセスすることによって、異常の原因を確認することができる。ウェブサイトでは、異常の前後の画像、例えば、動きのある侵入者の画像を確認できるので、ユーザは侵入者の存在を即座に確認できる。

## 【0030】

図示しないが、そのような場合には、ユーザの即座の対応を支援すべく適当な連絡先がウェブサイト上に用意される。例えば、ユーザは、侵入者の存在を確認したとき、その者を捕まえるべく、ウェブサイト（即ちウェブサーバ 11）を介して、即座に警備会社又は警察 99 に連絡することを可能にする。このとき、データサーバ 12 上の画像他のデータは警備会社又は警察 99 に情報として提供され得る。また、図示しないウェブサイトによれば、ユーザはウェブサイト上に警備会社又は警察等 99 以外の連絡先を登録することにより、他の関係者への連絡を自ら行うことも可能である。

## 【 0 0 3 1 】

本実施形態によるセキュリティシステム 1 0 0 の更なる特徴は、ユーザ端末 2 8 から通信装置 2 0 及びカメラ装置 2 1、2 2、2 3 を制御できることである。

「セキュリティオンモード」によれば、必ずしも通報があったときだけでなく、地震、洪水等の天災等が起こったときに、ユーザの側から状況を確認したいという要求もある。本実施形態はサーバ手段 1 0 を挟んでインターネット回線 8 0 を利用しこれを実現する。

## 【 0 0 3 2 】

ユーザは、必要な場合に自らのユーザ端末 2 8 からインターネットサービスプロバイダ 8 2 を介してインターネット回線 8 0 に入り、サーバ手段 1 0 による図示しないウェブサイトアクセスする。ウェブサイト上では、ユーザの認証を行うことにより、登録された通信装置 2 0 及びそれと通信可能なカメラ装置 2 1、2 2、2 3 を制御するためのメニューが用意される。ユーザは、適当なメニューを選択し、適当な操作を行うことにより、例えば、制御部 4 5 を遠隔的に制御することにより、カメラ装置 2 1、2 2、2 3 の監視角度範囲、設定モードの変更等を行うことができる。

## 【 0 0 3 3 】

更に、ユーザはウェブサイトアクセスし、各カメラ装置 2 1、2 2、2 3 に現在の画像の獲得を命令することができる。この場合、サーバ手段 1 0 は、予め与えられた情報等から適当なインターネットサービスプロバイダ 8 1 を介して通信装置 2 0 への通信を確立し、通信装置 2 0 に画像の獲得を命じる。通信装置 2 0 は各カメラ装置 2 1、2 2、2 3 に強制的に現在受像する画像のデータを送信することを命じる。その後、各カメラ装置 2 1、2 2、2 3 は、侵入者による異常が認められるのと同じデータの流れにより、サーバ手段 1 0 のデータサーバ手段 1 2 に画像データを保存する。このときサーバ手段 1 0 は、インターネット回線 8 0 を介した電子メール手段等によってユーザ端末 2 8 に向けて画像の獲得が完了した通知を行う。ユーザは、再度ウェブサイトアクセスすることにより更新された画像を確認することができる。

## 【 0 0 3 4 】

尚、上述の場合に、各カメラ装置 2 1、2 2、2 3 に現在の画像の獲得を命令するために、サーバ手段 1 0 が通信装置 2 0 に対して直接公衆電話回線による発信を行う方式を採用しても良い(図示せず)。この場合、通信装置 2 0 は、サーバ手段 1 0 からの通話信号又は発呼信号であることを確認できる手段を含む。通信装置 2 0 は、サーバ手段 1 0 からの信号であることを確認できた場合には、やはり上述の場合と同様に各カメラ装置 2 1、2 2、2 3 に画像データを送信することを命じることになる。次いで、画像データを受信した通信装置 2 0 は、インターネットサービスプロバイダ 8 1 を介してサーバ手段 1 0 への接続を確立し、画像データをサーバ手段 1 0 に提供する。その後の動作は上述の場合と同様である。初期段階におけるサーバ手段 1 0 から通信装置 2 0 への電話回線による通話時間は比較的短時間とすることができるので、通話によって生じるコストは比較的安価となる。

#### 【 0 0 3 5 】

ところで、「セキュリティオンモード」によれば、管理者が帰宅した際に、カメラ装置 2 1、2 2、2 3 が動作中であるという不都合を生じる。この場合、ユーザが監視されている場所 2 0 0 の外から通信装置 2 0 を無線手段等によりオフモードに変えることができるのが好ましい。またカメラ装置 2 1、2 2、2 3 がユーザの動きを検出して異常であると認識した場合に、所定時間内に通信装置 2 0 を操作することによりモードをオフモードに変えて異常信号のサーバ手段 1 0 への送信を停止させることも可能である。

#### 【 0 0 3 6 】

次に、「オフモード」、「セキュリティオンモード」以外の他の 2 つのモード「時間指定監視モード」及び「メッセージ送信モード」について説明する。これらは、必ずしも防犯のために設けられたものではない。

#### 【 0 0 3 7 】

「時刻指定監視モード」によれば、特定の対象を監視できるようカメラ装置を設置し、ユーザの指定する時間にその対象を観察する。このモードは例えばペット等の観察に使用される。例えばカメラ装置 2 1 は、予め指定された時刻にサーバ手段 1 0 から通信装置 2 0 を介して画像獲得の命令を受けることにより、その

ときの画像を獲得する。この画像データは、「セキュリティオンモード」の場合と同様に送信され、データベースサーバ12に保存される。従って、ユーザはウェブサイトアクセスすることによりその画像を確認することができる。このモードの場合では指定された時刻に限らず、ユーザが必要なときにウェブサイトから命令を送ることにより、画像を獲得することも可能である。

#### 【0038】

「メッセージ送信モード」によれば、例えば上述したように、カメラ装置21に設けられる音声検出手段49を併用して、通信手段20に設けられる図示しないコントロール装置の操作等により所定時間の間に画像と音声とでメッセージを構成し、これを上述の「セキュリティオンモード」と同様の方法でデータベースサーバ12上に保存させることができる。新しいメッセージの存在は上述の方法と同様にユーザ端末28への電子メール又は携帯電話等の手段によってユーザに伝えられる。ユーザはウェブサイトアクセスすることによりメッセージの内容を視覚又は聴覚により確認できる。画像は静止画に限らず短時間の動画であっても良い。

#### 【0039】

以上のように本発明の好適実施形態となるセキュリティシステムについて詳細に説明したが、これはあくまでも例示的なものであって、本発明を制限するものではなく、当業者によって様々な変形変更が可能である。

#### 【図面の簡単な説明】

##### 【図1】

本発明の好適実施形態となるセキュリティシステムの概略図。

##### 【図2】

図1のセキュリティシステムにおける4種類の動作モードを説明する図。

##### 【図3】

図1のセキュリティシステムにおけるカメラ装置及び通信装置の詳細な構成を示す概略図。

#### 【符号の説明】

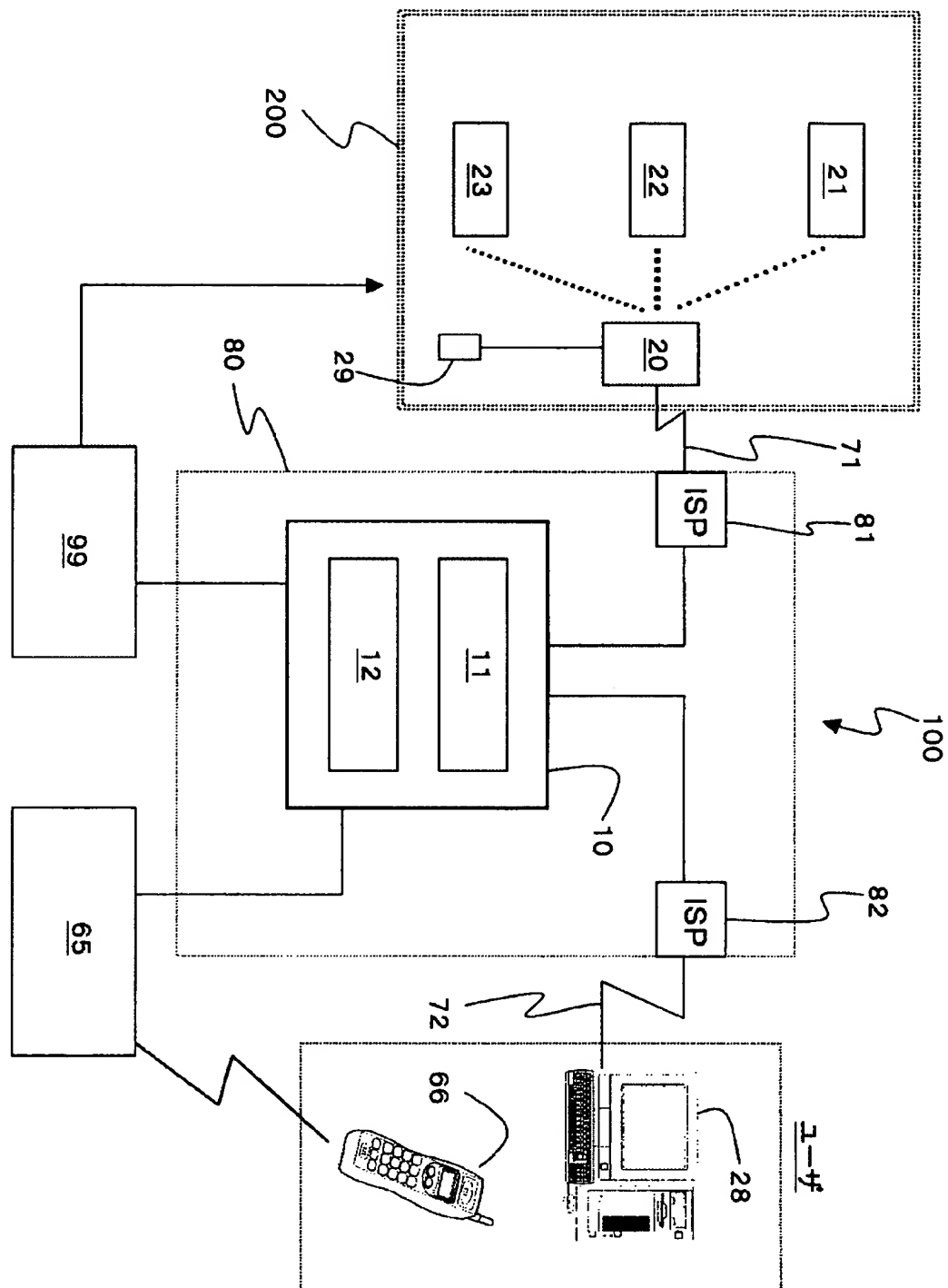
10

サーバ手段

1 1	ウェブサーバ
1 2	データベースサーバ
2 0	通信装置
2 1、2 2、2 3	カメラ装置
1 0 0	セキュリティシステム

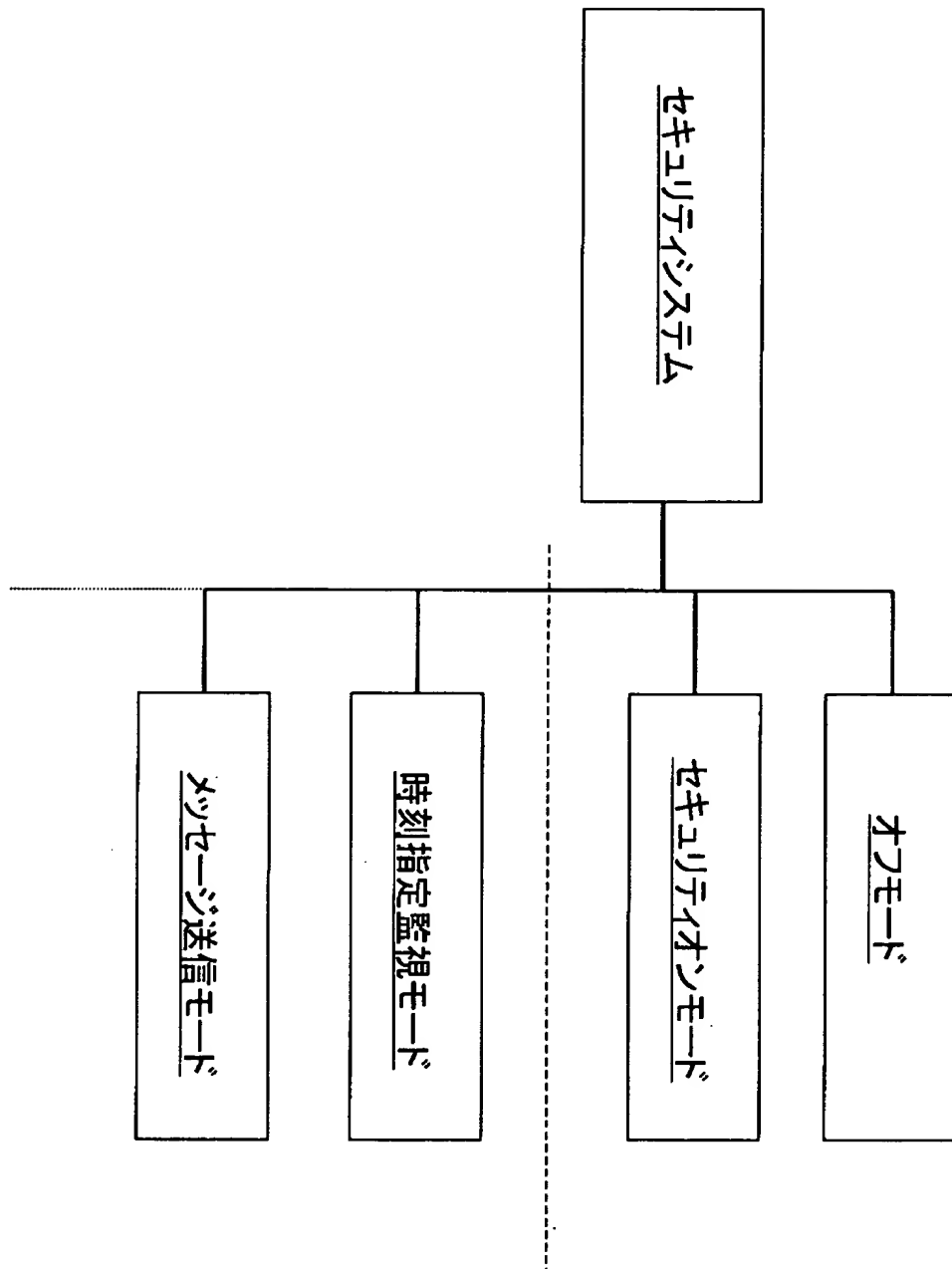
【書類名】 図面

【図 1】

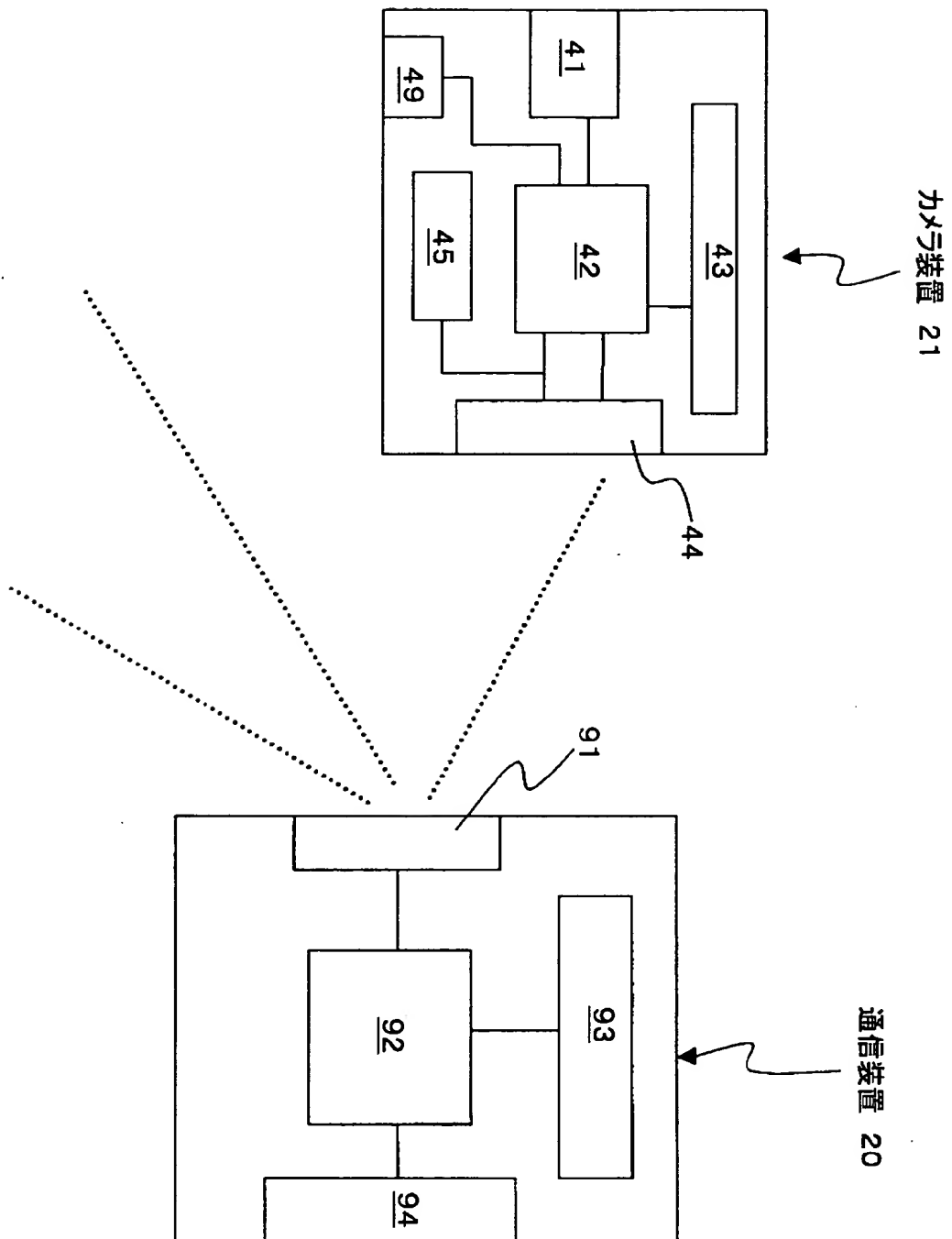




【図2】



【図 3】



【書類名】 要約書

【要約】

【課題】 正確な情報の効率的な伝達及び活用を比較的単純な構成で且つ低コストで実現することのできるセキュリティシステムを提供する。

【解決手段】 セキュリティシステム 1 0 0 によれば、ユーザにとって監視が必要とされる場所に複数のカメラ装置 2 1、2 2、2 3 及び通信手段 2 0 を有する。複数のカメラ装置 2 1、2 2、2 3 は、常時その場所を監視する。各カメラ装置 2 1、2 2、2 3 は、動き検出機能を有し、侵入者の動きが検出されたときのみ異常信号及び必要な画像情報を通信手段 2 0 に提供する。通信手段 2 0 は、その異常信号を受けたときのみインターネット回線 8 0 を使って情報センタとなるサーバ手段 1 0 に通信接続され、その際にカメラ装置 2 1、2 2、2 3 からの情報もサーバ手段 1 0 に送信される。サーバ手段 1 0 はユーザが予め選択した方法等によりユーザ他への自動通知を行う。通知を受けたユーザはサーバ手段 1 0 にアクセスして、異常に関する詳細な情報を画像として確認できる。

【選択図】 図 1

認 定 ・ 付 加 情 報

特許出願の番号	特願 2 0 0 0 - 3 6 5 9 1 5
受付番号	5 0 0 0 1 5 4 8 3 4 0
書類名	特許願
担当官	第四担当上席 0 0 9 3
作成日	平成 1 2 年 1 2 月 1 日

< 認定情報・付加情報 >

【提出日】	平成12年11月30日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [000121914]

1. 変更年月日	1999年11月 1日
[変更理由]	名称変更
住 所	東京都八王子市高倉町9番1号
氏 名	アジレント・テクノロジー株式会社